FORCEPOINT
POWERED BY Raytheon

Installation Guide

Advanced Malware Detection On-Premises Engine

v1.0

10900-A Stonelake Blvd, Quarry Oaks 1, Suite 350, Austin TX 78759

Published 2018

Contents

1 Introduction

Installation Guide | AMD OP Engine | v1.0

This guide describes the process to install the Advanced Malware Detection On-Premises Engine component on hardware provided by the customer.

The Engine component receives artifacts (i.e., executables and documents) from the Advanced Malware Detection On-Premises Manager. It runs these artifacts, and then returns analysis results back to the Manager (which then displays results to the users). The Engine is managed by the Manager. However, as an important part of the installation process, the Engine must be made known to the Manager.

2 Prerequisites

Installation Guide | AMD OP Engine | v1.0

Hardware

Advanced Malware Detection On-Premises Engine is a software solution that leverages your existing hardware. The following system requirements provide the minimum specifications for optimal performance and effectiveness.

- 1x Intel Xeon E5 6-core CPU
- 48 GB RAM
- 2x 1TB 7.2K RPM SATA disks (RAID 1)
- Dual PSU (highly recommended)
- ILO/LOM/DRAC (highly recommended)

Forcepoint also offers an option of purchasing a Dell PowerEdge R430 server that is suitable for hosting Advanced Malware Detection On-Premises Engine. Forcepoint delivers the server with the Advanced Malware Detection On-Premises Engine software pre-installed.

Network connectivity

The appliance needs to be able to connect to:

- log.MANAGER to TCP port 443.
- update.MANAGER to TCP port 443 and 8443
- update.MANAGER to UDP port 1194
- update.MANAGER to UDP port 123 for time synchronization.
- user.MANAGER to TCP port 443. It can be replaced with a local NTP server.

Note: MANAGER is replaced with the Advanced Malware Detection On-Premises Manager's Fully Qualified Domain Name (FQDN).

All the HTTPS connections (port 443) can be optionally routed though an explicit HTTP proxy.

License

Before starting the installation, the user has to acquire a license for the software. This is done by contacting the Forcepoint Support.

If you have already purchased the product, your license information can be found under the Products tab after you log on to the Forcepoint Support Portal. The following license information is provided:

- AMD Portal Username
- API Key
- API Token
- FQDN

Furthermore, you will need your Lastline Portal password. To retrieve this password:

1. Navigate to the Lastline Portal.
2. Click **Forgot your password?**
3. Follow the instructions provided on the Portal. You will need your Lastline Account Username.

License extensions

To renew an expired license, contact Forcepoint Sales. Once your request has been processed, your license expiration date will automatically be extended.

3 Installation Process

Installation Guide | AMD OP Engine | v1.0

The installation process for the Advanced Malware Detection On-Premises Engine consists of two steps. In the first step, the base system is installed. In the second step, basic configuration information is collected and the configuration is applied to the system.

If you purchased a Dell PowerEdge R430 server from Forcepoint with the Advanced Malware Detection On-Premises Engine software pre-installed, skip to *Registration and configuration*, page 5.

Base system installation

The Advanced Malware Detection On-Premises Engine uses Ubuntu 14.04.5 LTS as the underlying operating system. It uses an automated installation process that eliminates the need for user input. The installation is text-based; no graphical user interface is provided.

Before starting the installation, you must obtain an official copy of the latest Advanced Malware Detection On-Premises Engine ISO from Forcepoint. The image may be burned onto a bootable DVD, or simply mounted using the Dell iDRAC interface, if available.

To install Advanced Malware Detection On-Premises Engine, boot the system from the selected medium and let it run to completion. The installation is automatic and will only stop if it encounters a hardware error. The system will reboot twice, and then present you with a log on prompt.

Registration and configuration

The Advanced Malware Detection On-Premises Engine appliance should be connected to the Advanced Malware Detection On-Premises Manager's **eth1** port (2nd NIC). If there are multiple Advanced Malware Detection On-Premises Engines, a switch or private VLAN should be used to create a private network that connects to the Advanced Malware Detection On-Premises Manager's 2nd NIC.

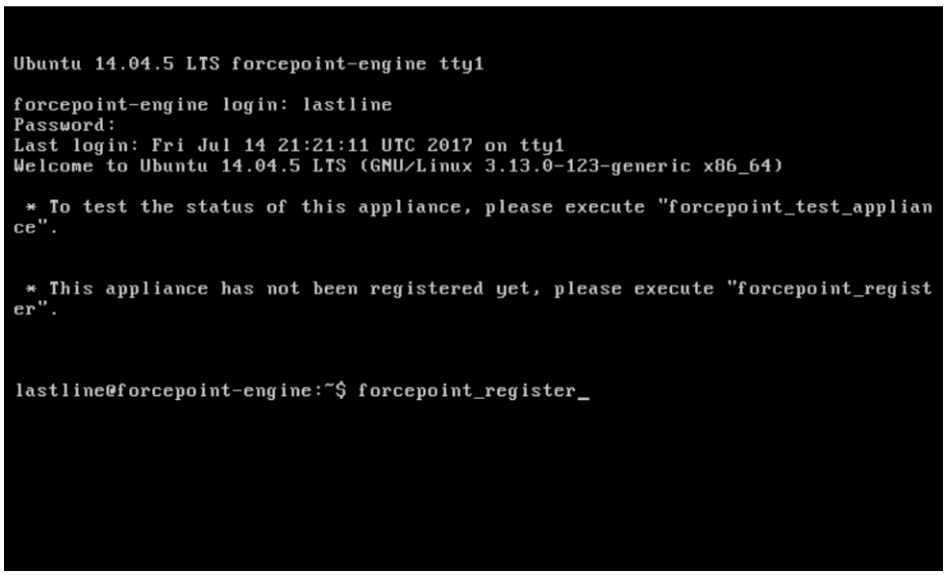
To register and apply the software configuration to the Advanced Malware Detection On-Premises Engine, log on to the console using

- username: **lastline**
- password: **lastline**

Note, it is possible to log on with the username and password only from a console.

Important
This is a default password that is available for all Advanced Malware Detection On-Premises Engine installations. It is highly recommended to change the default password to a password that is unique to your organization.

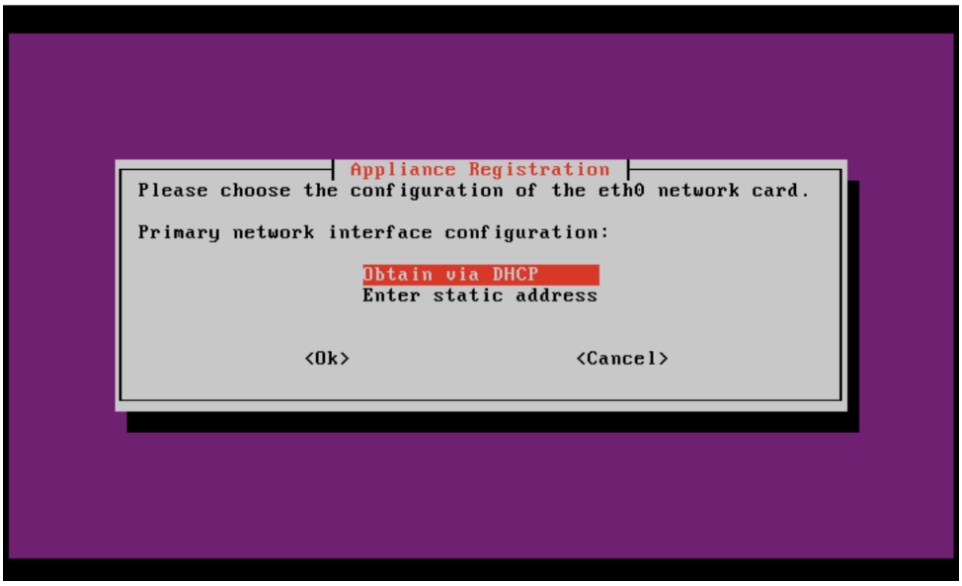
Execute **forcepoint_register**, which will start the guided registration and configuration process.



The registration process will give the user the opportunity to configure the network via DHCP or with a static IP address.

Forcepoint strongly recommends the use of DHCP. An IP in the range of 10.0.0.200-254 will be assigned to each Advanced Malware Detection On-Premises Engine on the private engine network. The Advanced Malware Detection On-Premises Engines will obtain IPs via DHCP from the Advanced Malware Detection On-Premises Manager over the engine network.

If static IPs are issued, use the 10.0.0.11-199 range.

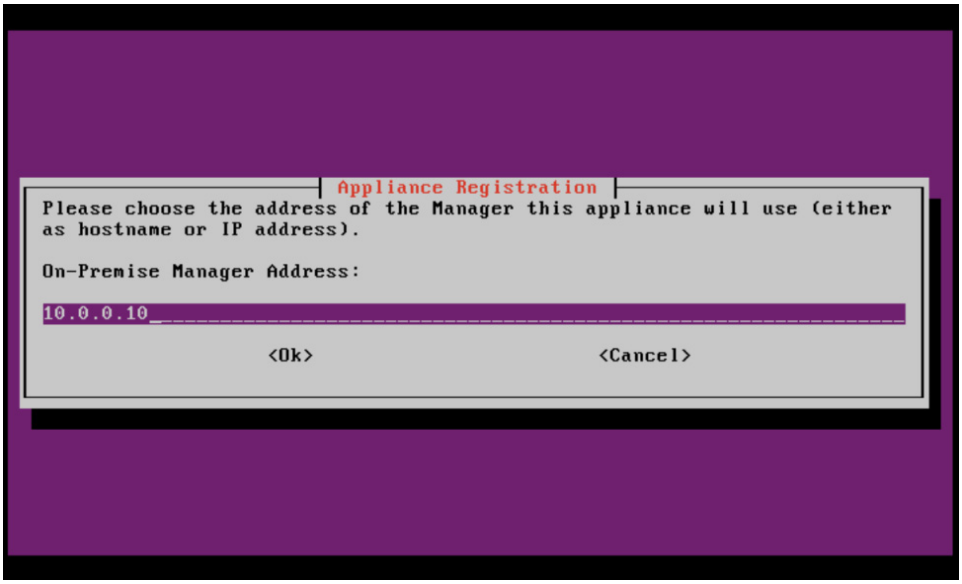


If an Advanced Malware Detection On-Premises Manager has been installed in the network, the user has to specify its domain name. For example, if the domain name of the Advanced Malware Detection On-Premises Manager is **amd-manager.mycompany.com**, then this name should be provided. Note that, as part of the installation of the Advanced Malware Detection On-Premises Manager, the names

- update.amd-manager.mycompany.com
- log.amd-manager.mycompany.com
- user.amd-manager.company.com

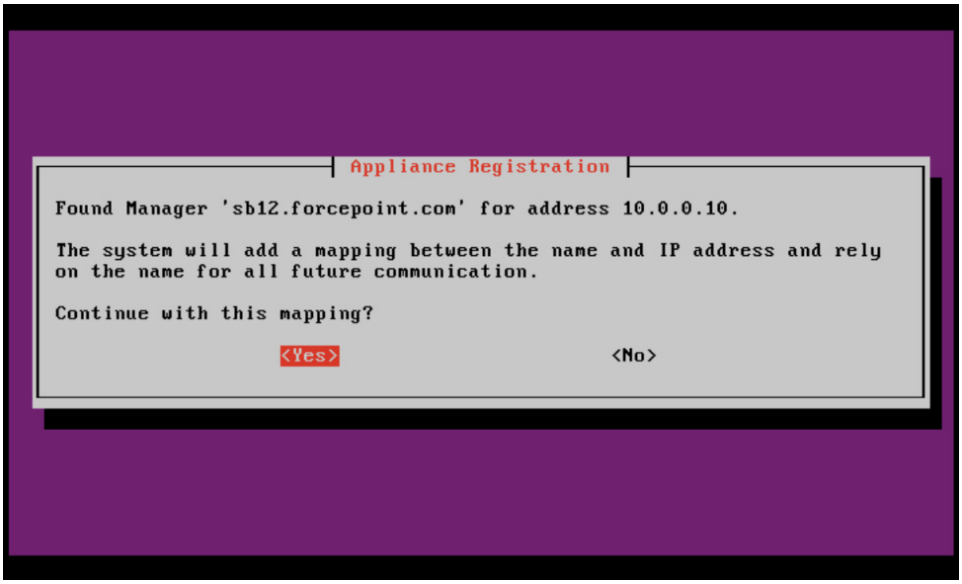
should have also been registered as aliases of **amd-manager.mycompany.com**.

In case an Advanced Malware Detection On-Premises Manager has been installed in the network, but no FQDN has been assigned to it (or the DNS server is not able to resolve its domain name), then the IP address of the Manager can be provided to the installer, as shown below.

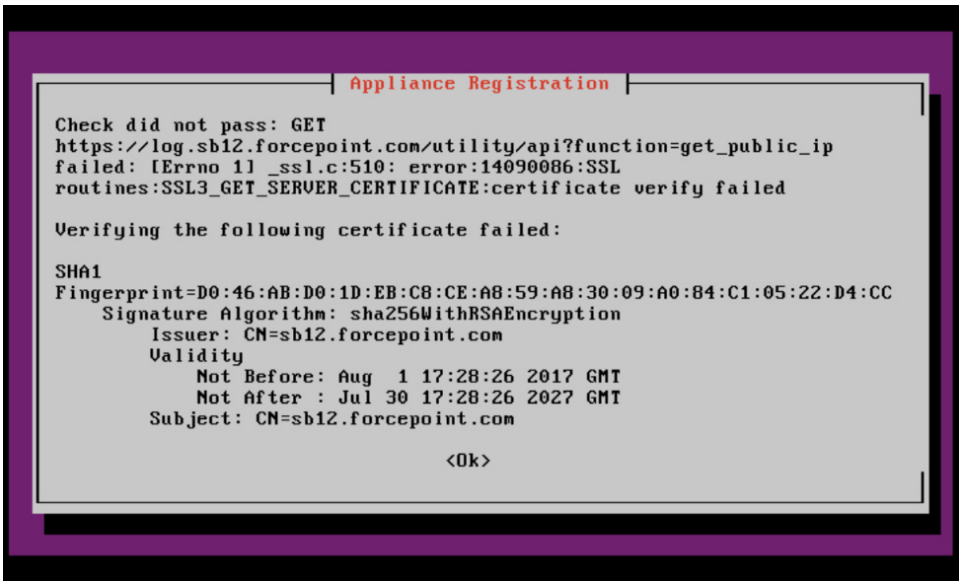


The Advanced Malware Detection On-Premises Manager's IP address has automatically been assigned to **10.0.0.10**. Enter this address when prompted for the Advanced Malware Detection On-Premises Manager's IP address.

At this point, the installer will try to configure the Advanced Malware Detection On-Premises Engine by using the IP address of the Advanced Malware Detection On-Premises Manager.

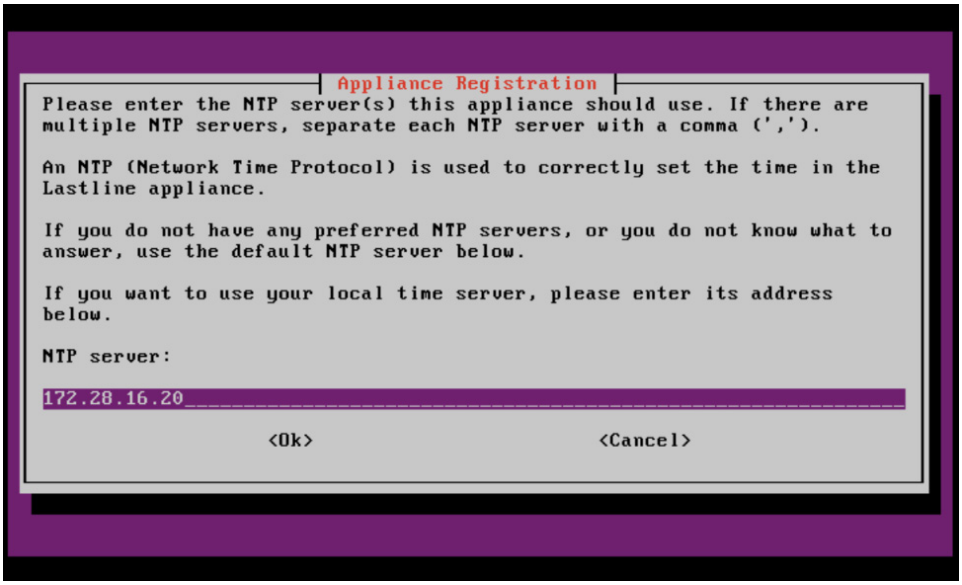


After you select **Yes**, you may see a certificate error page similar to the screen below:



Select **Ok** on this screen, then **Yes** on the next screen when asked to trust the certification. Verifying that the certificate failed will not negatively impact the Advanced Malware Detection On-Premises Engine registration process.

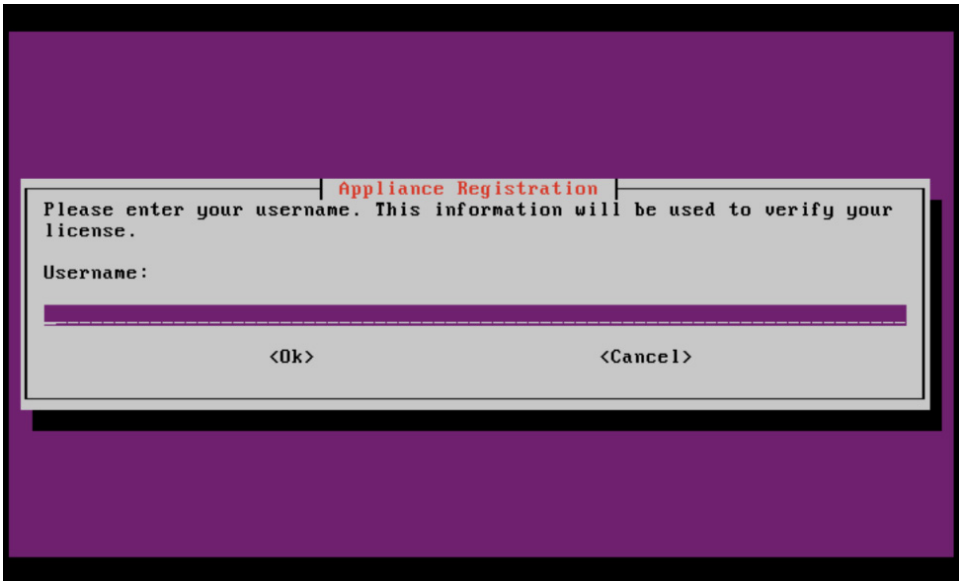
In the next step, the system will ask for a NTP server. Unless the use of a different NTP server is needed, the user can use the default value. The system must be able to reach the chosen NTP server over UDP port 123.

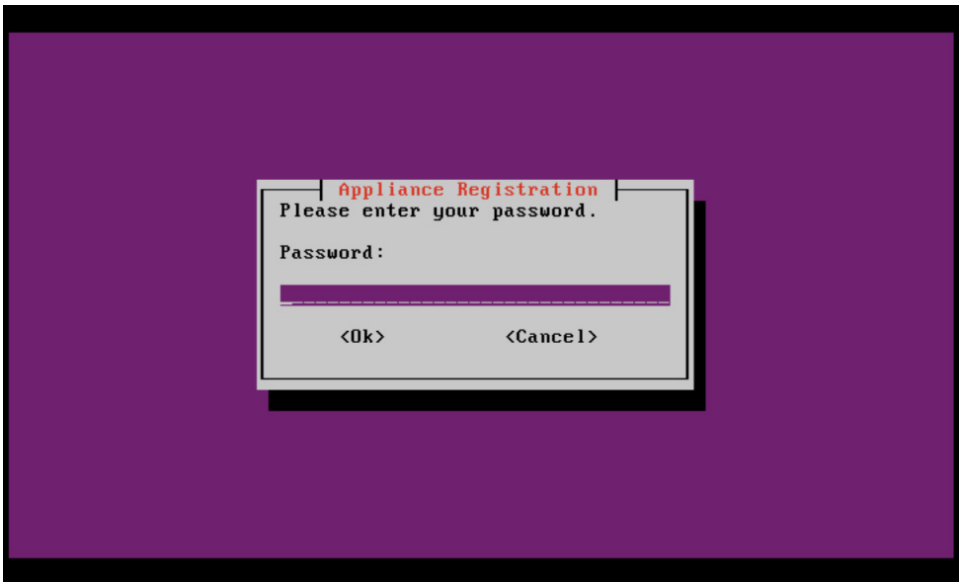


Select **Ok** to save the NTP server information.

You will then be prompted to verify your readiness to complete the configuration process. Select **Yes** to begin the system configuration and product registration. Internet access is required throughout this portion of the registration process.

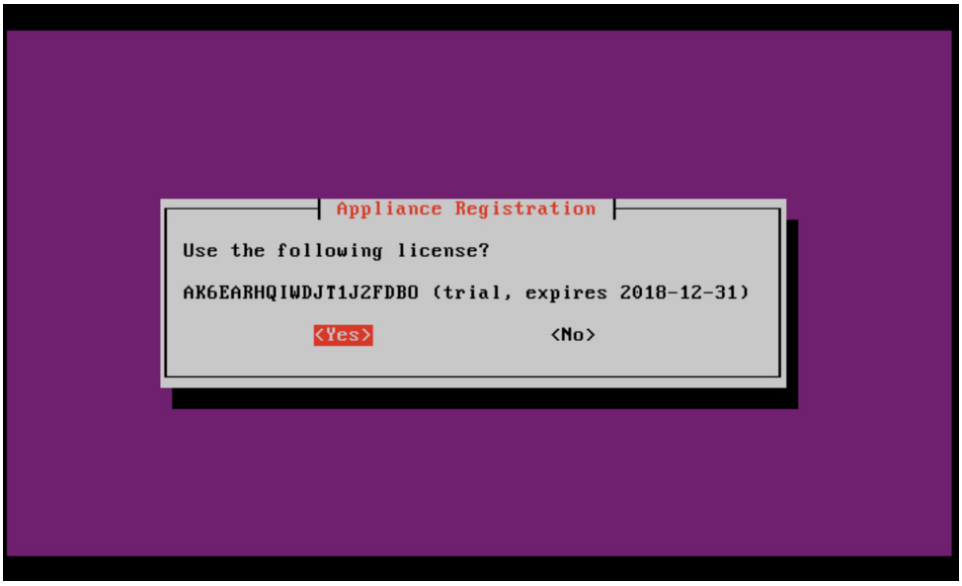
Next, provide the license information associated with this Advanced Malware Detection On-Premises Engine system. More precisely, enter the username and password provided during registration.





If the provided credentials are valid, you will be shown the available license keys and will be able to choose or approve a pre-selected choice.

If the list of license keys is not retrieved correctly, please contact Forcepoint Support, mentioning the corresponding error message.



If you select **No**, you will be asked if you want to restart the configuration process. Select **Yes** to restart the configuration, or **No** to stop the configuration process.

If the license information is correct, select **Yes**.

Now tests will be run to check hardware compatibility.

The setup program will now apply the configuration to the machine. This process may take several minutes (20-40) depending on network connectivity and system characteristics.

The registration has completed.

At this point, users can direct the browser to https://<<*IP address of AMD Engine*>> or https://<<*assigned FQDN*>> to access the user portal.

In case any error message is displayed, please refer to *Error handling*, page 13.

4 System Administration

Installation Guide | AMD OP Engine | v1.0

The Advanced Malware Detection On-Premises Engine is developed to require as little maintenance and administration as possible. The only action that might be required is to change the system's network configuration, as discussed below.

We also provide a troubleshooting guide that allows the administrator to ensure that everything works properly.

Advanced Malware Detection On-Premises Engine installation wizard

The easiest way to modify the system configuration is by re-running the Advanced Malware Detection On-Premises Engine installation wizard tool using the following command:

```
forcepoint_register
```

You will be able to change the latest configuration values provided the last time the installation wizard ran.

Error handling

If any error message is displayed when using **amd_setup**, please contact Forcepoint Support.

5 Software Upgrades

Forcepoint periodically releases appliance and software upgrades or hotfixes. Available updates will be communicated through email along with Release Notes and upgrade instructions.

If the software has automatic updates enabled, these updates will transparently be applied.

Automatic software updates are enabled by default upon installation. To disable automatic upgrades, or to manually upgrade an appliance with automatic updates disabled, log on to the web interface of the appliance itself and access the appliance configuration page from the Appliances tab.

6 Copyrights and Trademarks

Installation Guide | AMD OP Engine | v1.0

Published 2017
Printed in the United States of America

Copyrights and trademarks

Other acknowledgments

This Forcepoint product uses the third-party software listed in this file.